Äquivalenz der Sätze von Kronecker—Hensel und von Szekeres für die Ideale des Polynomringes einer Unbestimmten über einem kommutativen Hauptidealring mit Primzerlegung.

Von LADISLAUS RÉDEI in Szeged.

Es ist ein wichtiges, bisher in wenigen Fällen gelöstes Problem, daß man die sämtlichen verschiedenen Ideale eines Ringes angibt. Das kann z. B. so geschehen, daß man zu jedem Ideal des Ringes ein Erzeugendensystem eindeutig bestimmt. Auf diese Weise wurde das Problem für den Polynomring $R[x]$ über einem kommutativen Hauptidealring R mit Primzerlegung von KRONECKER—HENSEL [1][1]) gelöst. Diese haben in der Wahrheit nur den Spezialfall betrachtet, daß R der Ring der ganzen Zahlen ist, aber ihr Satz gilt samt Beweis auch für den gesagten allgemeinen Fall. Trotz der Wichtigkeit dieses Satzes scheint er in der „neuen" Algebra seinen gebührenden Platz nicht eingenommen zu haben, was zum großen Teil wohl dem Umstand zuzuschreiben ist, daß die Verfasser bei ihren Betrachtungen sich der (auch schon zurzeit etwas unmodernen) Sprache der „Modulsysteme" bedient haben. So war der Satz wohl auch Herrn SZEKERES unbekannt gewesen, als er für das Problem vor einigen Jahren eine neue Lösung veröffentlicht hatte; siehe SZEKERES [2]. Der Satz von SZEKERES lautet anders als der von KRONECKER—HENSEL. Beide Sätze verhalten sich zueinander so: Der Satz von SZEKERES ist kürzer gefaßt und somit eleganter, auch der Beweis ist einfacher, dagegen ist der Satz von KRONECKER—HENSEL mehr bis in die Einzelheiten ausgearbeitet, weshalb er für die Anwendungen mehr geeignet zu sein scheint.

Es wird sich zeigen, das der Satz von SZEKERES sich leicht in den von KRONECKER—HENSEL umformen läßt. Auf diesem Wege entsteht aus dem vorigen ein Beweis für den letzteren, der leichter ist als der ursprüngliche.[2])

Wir wählen irgendwie ein Repräsentantensystem $\mathfrak{R}$ der Klassen der von 0 verschiedenen assoziierten Elemente von R fest, schreiben aber vor, $\mathfrak{R}$ daß

[1]) Mit [ ] verweisen wir auf das Literaturverzeichnis am Schluß unserer Arbeit.

[2]) Eine der heutigen Sprache der Algebra angepaßte Ausarbeitung des Kronecker—Henselschen Beweises findet sich bei RÉDEI [3].

das Einselement 1 von R enthält. (Das bedeutet, daß die Klasse der Einheiten durch 1 repräsentiert wird.) Ferner wählen wir für jedes Element $\varrho(\in \mathfrak{R})$ ein Repräsentantensystem $\mathfrak{R}(\varrho)$ der Restklassen mod ϱ irgendwie fest, schreiben aber vor, daß jedes $\mathfrak{R}(\varrho)$ die 0 enthält.

Eine erste Übersicht über die Ideale von $R[x]$ läßt sich folgenderweise gewinnen. (Das Nullideal lassen wir durchweg außer Acht.) Jedes Ideal von $R[x]$ läßt sich eindeutig als ein Produkt $f(x)\mathfrak{a}$ schreiben, wobei $f(x)$ in $R[x]$ und der Anfangskoeffizient von $f(x)$ in $\mathfrak{R}$ gehört, ferner $\mathfrak{a}$ ein *primitives* Ideal in $R[x]$ ist, dessen Elemente nämlich relativ prim sind.

Der Satz von SZEKERES [9] S. 385 lautet so:

Man gebe endlich viele Elemente[3])

$$\varrho_1, \ldots, \varrho_m (\in \mathfrak{R}) \qquad (m \geqq 0; \quad \varrho_m \neq 1) \tag{1}$$

und zu jedem ϱ_k weitere k Elemente

$$\varrho_{ki} (\in \mathfrak{R}(\varrho_k)) \qquad (i = 0, \ldots, k-1; \quad k = 1, \ldots, m) \tag{2}$$

an. Dann werden durch die rekursive Definition

$$g_0(x) = \varrho_1 \ldots \varrho_m, \quad \varrho_k g_k(x) = x g_{k-1}(x) + \sum_{i=1}^{k-1} \varrho_{ki} g_i(x) \qquad (k = 1, \ldots, m) \tag{3}$$

lauter Polynome $g_0(x), \ldots, g_m(x)$ in $R[x]$ angegeben. Dabei ist $g_k(x)$ vom Grade k und von der Form

$$g_k(x) = \varrho_{k+1} \ldots \varrho_m (x^k + \ldots) \qquad (k = 1, \ldots, m). \tag{4}$$

Die zu den verschiedenen Systemen (1), (2) gehörenden

$$\mathfrak{a} = (g_0(x), \ldots, g_m(x)) \tag{5}$$

sind eben die sämtlichen verschiedenen primitiven Ideale von $R[x]$.

Bemerkung. Im Fall $m = 0$ soll $g_0(x) = \varrho_1 \ldots \varrho_m = 1$ verstanden werden, weshalb dann (5) in $\mathfrak{a} = R[x]$ übergeht. Es ist eine leichte Folgerung des Satzes, daß der Anfangskoeffizient $\varrho_{k+1} \ldots \varrho_m$ von $g_k(x)$ der größte gemeinsame Teiler der Anfangskoeffizienten aller Polynome in $\mathfrak{a}$ vom Gerade k ist. Offenbar ist dann m das Minimum der Gradzahlen aller Hauptpolynome in $\mathfrak{a}$; Hauptpolynom heißt ein Polynom mit dem Anfangskoeffizienten 1.

Um nun obigen Satz umzuformen betrachten wir die von 1 verschiedenen Glieder der Folge (1). Ihre Indizes bilden eine Folge

$$n_1 < n_2 < \cdots < n_r (= m) \qquad (r \geqq 1). \tag{6}$$

Man verwende für die betrachteten Glieder von (1) die kürzere Bezeichnung

$$\varrho_{n_i} = \sigma_i \qquad (i = 1, \ldots, r) \tag{7}$$

[3]) Im fall $m = 0$ bedeutet (1) das leere System, weshalb die Bedingung $\varrho_m \neq 1$ nur im Fall $m > 0$ in Kraft tritt. Bei SZEKERES [2] fehlt die Bedingung $\varrho_m \neq 1$, was ein offenbares Versehen ist.

und setze

$$F_i(x) = g_{n_i}(x) \qquad (i = 0, \ldots, r; \quad n_0 = 0). \tag{8}$$

Insbesondere gilt nach (3_1) $F_0(x) = \varrho_1 \ldots \varrho_m$, also

$$F_0(x) = \sigma_1 \ldots \sigma_r. \tag{9}$$

Betrachten wir ein von allen n_i verschiedenes $k (= 1, \ldots, m)$. Für dieses gilt $\varrho_k = 1$, weshalb $\mathfrak{R}(\varrho_k)$ das einzige Element 0 hat. Hieraus folgt nach (2) $\varrho_{ki} = 0$ $(i = 0, \ldots, k-1)$. Dies ergibt nach (3_2) durch Induktion

$$g_i(x) = x^{i-n_j} g_{n_j}(x) = x^{i-n_j} F_j(x) \qquad (n_j \leqq i < n_{j+1}; \quad j = 0, \ldots, r-1), \tag{10}$$

wobei wir auch (8) berücksichtigt haben. Da nach (6) und (8) insbesondere $g_m(x) = F_r(x)$ ist, so folgt aus (5) und (10):

$$\mathfrak{a} = (F_0(x), \ldots, F_r(x)). \tag{12}$$

Ferner läßt sich (3_2) für $k = n_1, \ldots, n_r$ wegen (7), (8) und (10) in der Form

$$\sigma_{l+1} F_{l+1}(x) = x^{n_{l+1}-n_l} F_l(x) + \sum_{i=0}^{n_{l+1}-1} \varrho_{n_{l+1}i} g_i(x) \qquad (l = 0, \ldots, r-1)$$

schreiben. Wegen (10) ergibt sich hieraus nach leichter Umformung:

$$\sigma_{l+1} F_{l+1}(x) = x^{n_{l+1}-n_l} F_l(x) + \sum_{k=0}^{l} F_k(x) \sum_{i=n_k}^{n_{k+1}-1} \varrho_{n_{l+1}i} x^{i-n_k} \qquad (l = 0, \ldots, r-1).$$

Die innere Summe ist ein Polynom $g_{kl}(x)$ vom Grade $< n_{k+1} - n_k$, dessen Koeffizienten nach (2) und (7) aus $\mathfrak{R}(\sigma_{l+1})$ genommen sind. Hiernach gilt

$$\sigma_{l+1} F_{l+1}(x) = (x^{n_{l+1}-n_l} + g_{ll}(x)) F_l(x) + \sum_{k=0}^{l-1} g_{kl}(x) F_k(x) \qquad (l = 0, \ldots, r-1).$$

Schreibt man noch $f_{k+1\,l+1}(x)$ statt g_{kl}, so erscheint endlich der Satz von SZEKERES in folgender Form:

Man gebe *erstens* ganze Zahlen

$$0 = n_0 < n_1 < \cdots < n_r \qquad (r \geqq 0), \tag{13}$$

zweitens Elemente

$$\sigma_1, \ldots \sigma_r (\in \mathfrak{R}), \tag{14}$$

drittens Polynome

$$f_{kl}(x) \qquad (1 \leqq k \leqq l \leqq r) \tag{15}$$

mit Koeffizienten aus $\mathfrak{R}(\varrho_l)$ und vom Grade $< n_k - n_{k-1}$ an und bestimme

die Polynome $F_0(x), \ldots, F_r(x)$ rekursiv aus den Gleichungen

$$
\begin{aligned}
& F_0(x) = \sigma_1 \ldots \sigma_r, \\
& \sigma_1 F_1(x) = (x^{n_1} + f_{11}(x))\, F_0(x), \\
(16)\quad & \sigma_2 F_2(x) = f_{12}(x)\, F_0(x) + (x^{n_2 - n_1} + f_{22}(x))\, F_1(x), \\
& \quad\vdots \\
& \sigma_r F_r(x) = f_{1r}(x)\, F_0(x) + f_{2r}(x)\, F_1(x) + \cdots + (x^{n_r - n_{r-1}} + f_{rr}(x))\, F_{r-1}(x).
\end{aligned}
$$

Diese $F_i(x)$ liegen in $R[x]$. Die zu den Systemen (13), (14), (15) gehörenden

$$\mathfrak{a} = (F_0(x), \ldots, F_r(x)) \tag{17}$$

sind eben die sämtlichen verschiedenen Ideale von $R[x]$.

Bemerkung. Dies ist der Satz von KRONECKER—HENSEL [1] in verallgemeinerter Form. KRONECKER—HENSEL bewiesen nämlich den Satz nur für primäre primitive Ideale $\mathfrak{a}$, d. h. für den Fall, daß $F_0(x) = \varrho_1 \ldots \varrho_r$ die Potenz eines Primelementes von R ist. Im Prinzip genügt das, da die primitiven Ideale von $R[x]$ sich eindeutig als Produkt (oder Durchschnitt) von primären Idealen erzeugen lassen, trotzdem kann oft auch obige verallgemeinerte Form des Satzes vom Vorteil sein. Die weitere Verallgemeinerung besteht darin, wie gesagt, daß bei KRONECKER—HENSEL nur der Ring der ganzen Zahlen statt eines beliebigen Euklidischen Ringes R betrachtet wird. (In diesem Spezialfall kann natürlich für R die Menge der positiven ganzen Zahlen und für $\mathfrak{R}(a)$ $(a \in \mathfrak{R})$ das Restsystem $0, \ldots, a-1 \bmod a$ genommen werden.) Es soll betont werden, daß wohl beide Sätze, nämlich der von KRONECKER—HENSEL und der von SZEKERES, sehr einfach alle verschiedenen Ideale von $R[x]$ bestimmen, daß aber es sich in ihnen wegen der willkürlichen Wahl von $\mathfrak{R}$, $\mathfrak{R}(\varrho)$ um keine invariante Bestimmung handelt. (Absolute Invarianten sind die Zahlen $n_1, \ldots, n_r$ (in (13).) Man bemerke auch, daß (17) im allgemeinen keine „kürzeste Darstellung" von $\mathfrak{a}$ ist. Z. B. betrachten wir nämlich das durch zwei Elemente erzeugte Ideal $\mathfrak{a} = (x^5, x^3 - p^3)$, wobei jetzt R der Ring der ganzen Zahlen und p eine Primzahl ist. Man sieht leicht, daß jetzt (17) als $\mathfrak{a} = (x^3 - p^3, p^3 x^2, p^5)$ lautet, wobei drei Erzeugende auftreten. Diese „Abundanz" der Darstellung (17) ist aber gegenüber ihrer Eleganz kein ernster Nachteil. Man bemerke noch, daß sich (16) mit Hilfe von Matrizen auch so schreiben läßt:

$$F_0(x) = \sigma_1 \ldots \sigma_r,$$

$$
(17)\quad \begin{pmatrix} \sigma_1 F_1(x) \\ \vdots \\ \sigma_r F_r(x) \end{pmatrix} = \begin{pmatrix} x^{n_1} + f_{11}(x) & & 0 & \\ f_{12}(x) & x^{n_2 - n_1} + f_{22}(x) & & \\ \vdots & & & \\ f_{1r}(x) & f_{2r}(x) & \ldots & x^{n_r - n_{r-1}} + f_{rr}(x) \end{pmatrix} \begin{pmatrix} F_0(x) \\ \vdots \\ F_{r-1}(x) \end{pmatrix}.
$$

Im ersten Faktor auf der rechten Seite der zweiten Gleichung haben die Polynome $f_{kl}(x)$ in der k-ten Zeile einen Grad $< n_k - n_{k-1}$, die in der l-ten Spalte haben lauter Koeffizienten aus $\mathfrak{R}(\varrho_l)$.

Literaturverzeichnis.

[1] Kronecker—Hensel, *Vorlesungen über Zahlentheorie* (Leipzig, 1901).
[2] Szekeres, G., A canonical basis for the ideals of a polynomial domain, *Amer. Math. Monthly*, 59 (1952), 379—386.
[3] Rédei L., *Algebra* I (Budapest, 1954).

(Eingegangen am 10. Dezember 1956.)